

# Содержание

<b>Работа с NAT Flow. Как найти абонента за NAT .....</b>	<b>3</b>
<b>Пример работы с abuse letters .....</b>	<b>3</b>
Шаг 1. Ищем в письме .....	3
Шаг 2. Ищем активность абонента в GUI СКАТ .....	4



# Работа с NAT Flow. Как найти абонента за NAT



Для работы данной функциональности необходимы следующие компоненты:  
[Модуль QoE Stor](#) и [Интерфейс управления СКАТ DPI](#).  
Описание настройки NAT в QoE: [Конфигурация NAT Flow](#)

## Пример работы с abuse letters

Ищем конкретного абонента, на которого пришел внешний abuse.

В письме с abuse, как правило, приведен «белый» адрес из NAT-пула, требуется понять кто из абонентов в известное время за этим NAT-пулом ходил на ресурс, где зафиксирована вирусная активность.

Нужно сделать **2 шага** — найти в abuse письме необходимые признаки и по ним в GUI СКАТ идентифицировать абонента.

### Шаг 1. Ищем в письме

1. Адрес из своего NAT-пула (source IP).
2. Адрес атакуемого ресурса (destination IP)
3. Время активности на атакуемом ресурсе (с учетом часовых поясов!)

- **Пример 1.**

```
From: "EGP Abuse Dept." <abuse-notify+32977_45.199.184.208.45@abuse.espresso-gridpoint.net>
Date: Sun Feb 19 2023 18:37:17 GMT+0000 (Coordinated Universal Time)
To: <abuse@cloudinnovation.org>, <tech@cloudinnovation.org>
Subject: [ EGP Cloudblock RBL / 1676831816.32977 | [ probe/scan/virus/trojan ] 45.199.184.208 (PTR: -) (ALERT: extremely problematic /24, 32-63 abusive hosts)
```

```
===== X-ARF Style Summary =====
Date: 2023-02-19T19:36:56+01:00
Source: 45.199.184.208
Type of Abuse: PortsCan/Malware/Intrusion Attempts
Logs: 19:36:48.510541 rule 0/0(match): block in on vmx0: 45.199.184.208.42205 > 91.190.98.8.59891 Flags [S], seq 3517664982, win 0, options [mss 1412], length 0
----- To whom it may concern, 45.199.184.208 is reported to you for performing unwanted activities toward our
```

- **Пример 2.**

```
Below is an overview of recently recorded abusive activity from 45.195.93.8/32
-----
Source IP / Targeted host / Issue processed @ / Log entry (see notes below)
----- * 45.195.93.8 tpc-022.mach3builders.nl 2023-01-30T15:45:15+01:00 15:45:12.435802 rule 0/0(match): block in on vmx0:
45.195.93.8.40422 > 91.190.98.11.445 Flags [S], seq 2611011070, win 0, options [mss 1412], length 0
* 45.195.93.8 tpc-022.mach3builders.nl 2023-01-30T15:45:14+01:00 15:45:11.870278 rule 0/0(match): block in on vmx0: 45.195.93.8.40422 > 91.190.98.11.445: Flags [S], seq 2611011070, win 0, options [mss 1412], length 0
```

Еще из полезного в письме может быть:

1. Причина abuse

Date: 2023-02-27T00:53:34+01:00

Source: 45.199.184.192

Type of Abuse: PortsCan/Malware/Intrusion Attempts

Logs: 00:53:29.425121 rule 0/0(match): block in on vmx0: 45.199.184.192.65001 > 91.190.98.8.59891: Flags [S], seq 3803861910, win 0, options [mss 1412], length 0

2. История abuse (если активность была неоднократной)

The reported IP address 45.199.184.192 is part of 45.199.184.0/24;  
33 of this network's 256 IP addresses (12.89%) were abusive in the last 90 days

### Host Last logged attempt (Netherlands time zone)

45.199.184.1 (2022-12-24T20:58:33+01:00)  
45.199.184.3 (2023-01-22T18:20:44+01:00)  
45.199.184.4 (2023-01-03T16:19:43+01:00)  
45.199.184.13 (2022-12-22T06:00:34+01:00)

Это может помочь понять масштаб проблемы и выявлять аналогичные проблемы в сети.

## Шаг 2. Ищем активность абонента в GUI СКАТ

Задача — определить по логам, какой абонент за NAT-пулом (source IP), указанным в письме, в это время обращался к адресу destination IP.

Перед началом поиска стоит проверить 2 факта:

1. Данный NAT-пул заведен на CG-NAT СКАТ.

The screenshot shows the VAS Experts SSG control interface. On the left, there is a sidebar with various service categories like Performance, Configuration, and Services. The 'Services' category is highlighted with a blue background and has a red arrow pointing to it. In the main content area, the 'CG-NAT' tab is selected, indicated by a red arrow. The 'Profiles' section shows a table with two rows: 'office-test' and 'nse'. The 'nse' row is expanded, showing a 'Description' field with 'cgnat', a 'Type' field with 'CGNAT', and a 'NAT IP pool' field with '187.86.164.0/27'. A red arrow points to the 'NAT IP pool' field. To the right, there is a 'Profile status' table and a 'Status' table showing session counts for various IP addresses.

2. Время хранения логов NAT захватывает время abuse-активности. Посмотреть и настроить

The screenshot shows the W3 Experts interface with the following navigation path: **Administrator** > **QoS configuration**. The left sidebar highlights the **Administrator** section, which includes **Equipment**, **QoS configuration** (selected), **QoS logs**, **QoS switch**, **QoS traffic configuration**, **QoS filter logs**, **Capture configuration**, **Capture template**, **Capture logs**, and **Hardware SSH terminal**.

The main content area displays the **QoS lifetime settings** configuration page. It lists several parameters with their current values:

- QoS stor cache lifetime in seconds (QOSSTOR\_CACHE\_LIFE\_TIME\_SEC)**: 3600
- QoS stor main log lifetime in hours (QOSSTOR\_MAIN\_LOG\_PARTITIONS\_LIFE\_TIME\_HOUR)**: 2
- QoS stor aggregated log lifetime in days (QOSSTOR\_AGG\_LOG\_PARTITIONS\_LIFE\_TIME\_DAYS)**: 14
- QoS stor fullflow main log lifetime in hours (QOSSTOR\_FULLFLOW\_MAIN\_LOG\_PARTITIONS\_LIFE\_TIME\_HOUR)**: 2
- QoS stor fullflow aggregated log lifetime in days (QOSSTOR\_FULLFLOW\_AGG\_LOG\_PARTITIONS\_LIFE\_TIME\_DAYS)**: 14
- QoS stor clickstream main log lifetime in hours (QOSSTOR\_CLICKSTREAM\_MAIN\_LOG\_PARTITIONS\_LIFE\_TIME\_HOUR)**: 2
- QoS stor clickstream aggregated log lifetime in days (QOSSTOR\_CLICKSTREAM\_AGG\_LOG\_PARTITIONS\_LIFE\_TIME\_DAYS)**: 14
- QoS stor NAT main log lifetime in hours (QOSSTOR\_NAT\_MAIN\_LOG\_PARTITIONS\_LIFE\_TIME\_HOUR)**: 2
- QoS stor NAT aggregated log lifetime in days (QOSSTOR\_NAT\_AGG\_LOG\_PARTITIONS\_LIFE\_TIME\_DAYS)**: 14
- QoS stor GTP main log lifetime in hours (QOSSTOR\_GTP\_MAIN\_LOG\_PARTITIONS\_LIFE\_TIME\_HOUR)**: 2
- QoS stor GTP aggregated log lifetime in days (QOSSTOR\_GTP\_AGG\_LOG\_PARTITIONS\_LIFE\_TIME\_DAYS)**: 14

Red arrows point to the values for the **QoS stor NAT aggregated log lifetime in days** (14) and the **QoS stor GTP aggregated log lifetime in days** (14).

Далее в GUI CKAT необходимо открыть раздел NAT flow, выбрать период, завести source и destination IP.

WIS Experts

Wi-Fi analytics > NAT flow

Search

Subscription status: Normal 20 days

Period: 03/03/2023 11:11 - 03/03/2023 11:11  For all Wi-Fi devices

**NAT flow aggregated log**

Time	Source IP	Source port	Destination	Destination	Port NAT	Port net	Login	Session
<input type="button" value="Q_Flow"/>	<input type="button" value="Q_Filter"/>	<input type="button" value="Q_Flow"/>	<input type="button" value="Q_Flow"/>	<input type="button" value="Q_Filter"/>	<input type="button" value="Q_Flow"/>	<input type="button" value="Q_Filter"/>	<input type="button" value="Q_Flow"/>	<input type="button" value="Q_Flow"/>
Data not found								

Filter	Operator	Value
<input type="checkbox"/> off	Source IPv4-address	<input type="text"/>
<input type="checkbox"/> off	Source port	<input type="text"/>
<input type="checkbox"/> off	Destination IPv4-address	<input type="text"/>
<input type="checkbox"/> off	Destination port	<input type="text"/>
<input checked="" type="checkbox"/> or	Port not source IPv4-address	<input type="text"/> 45.192.194.192
<input type="checkbox"/> off	Port not source port	<input type="text"/>
<input type="checkbox"/> off	Login	<input type="text"/>
<input type="checkbox"/> off	Protocol	<input type="text"/>
<input type="checkbox"/> off	Device type	<input type="text"/>

8-8 of 0  100



С найденным абонентом нужно произвести необходимые действия для профилактики дальнейших abuse.